ETSI TR 103 305-1 V3.1.1 (2018-09)

CYBER;
Critical Security Controls for Effective Cyber Defence;
Part 1: The Critical Security Controls

Reference
RTR/CYBER-0034-1

Keywords
cyber security, cyber-defence, information assurance

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

The present document is part 1 of a multi-part deliverable covering the Critical Security Controls for Effective Cyber Defence, as identified below:

Part 1: **"The Critical Security Controls";**

Part 2: "Measurement and auditing";

Part 3: "Service Sector Implementations";

Part 4: "Facilitation Mechanisms";

Part 5: "Privacy enhancement".

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The present document captures and describes the prioritized set of actions that collectively form a defence-in-depth set of best practices that mitigate the most common attacks against systems and networks. These actions are specified by ETSI in the present document the Critical Security Controls (CSC) which are developed and maintained by the Center for Internet Security (CIS) as an independent, expert, global non-profit organization. The CIS provides ongoing development, support, adoption, and use of these Critical Security Controls [i.1]. The Controls reflect the combined knowledge of actual attacks and effective defences of experts from every part of the cyber security ecosystem. This ensures that the Controls are an effective and specific set of technical measures available to detect, prevent, respond, and mitigate damage from the most common to the most advanced of those attacks.

The Controls are not limited to blocking the initial compromise of systems, but also address detecting already compromised machines and preventing or disrupting attackers' follow-on actions. The defences identified through these Controls deal with reducing the initial attack surface by hardening device configurations, identifying compromised machines to address long-term threats inside an organization's network, disrupting attackers' command-and-control of implanted malicious code, and establishing an adaptive, continuous defence and response capability that can be maintained and improved. The five critical tenets of an effective cyber defence system as reflected in the Critical Security Controls are:

- Offense informs defence: Use knowledge of actual attacks that have compromised systems to provide the foundation to continually learn from these events to build effective, practical defences. Include only those controls that can be shown to stop known real-world attacks.
- Prioritization: Invest first in Controls that will provide the greatest risk reduction and protection against the most dangerous threat actors, and that can be feasibly implemented in a computing environment.
- Measurements and Metrics: Establish common metrics to provide a shared language for executives, IT specialists, auditors, and security officials to measure the effectiveness of security measures within an organization so that necessary adjustments can be identified and implemented quickly.
- Continuous diagnostics and mitigation: Carry out continuous measurement to test and validate the effectiveness of current security measures, and to help drive the priority of next steps.
- Automation: Automate defences so that organizations can achieve reliable, scalable, and continuous measurements of their adherence to the Controls and related metrics.

Introduction

The evolution of cyber defence is increasingly challenging. Massive data losses, theft of intellectual property, credit card breaches, identity theft, threats to privacy, denial of service - these have become endemic. Access exists to an extraordinary array of security tools and technology, security standards, training and classes, certifications, vulnerability databases, guidance, best practices, catalogues of security controls, and countless security checklists, benchmarks, and recommendations.

But all of this technology, information, and oversight has become a veritable "Fog of More:" competing options, priorities, opinions, and claims that can paralyze or distract an enterprise from vital action. Business complexity is growing, dependencies are expanding, users are becoming more mobile, and the threats are evolving. New technology brings great benefits, but it also means that data and applications are now distributed across multiple locations, many of which are not within the organization's infrastructure. In this complex, interconnected world, no enterprise can think of its security as a standalone problem.

Focus is needed to establish priority of action, collective support, and keeping knowledge and technology current in the face of rapidly evolving problems and an apparently infinite number of possible solutions. The most critical areas need to be addressed and the first steps taken toward maturing risk management programs. This includes a roadmap of fundamentals, and guidance to measure and improve the implementation defensive steps that have the greatest value. These issues led to, and drive, the Critical Security Controls. The value is determined by knowledge and data - the ability to prevent, alert, and respond to the attacks that are plaguing enterprises today.

Initiating Implementation

Some of the Critical Security Controls, in particular CSC 1 through CSC 6, are essential to success and should be considered among the very first things to be done. This is the approach taken by, for example, the DHS Continuous Diagnostic and Mitigation (CDM) Program. A similar approach is recommended by the Australian Signals Directorate (ASD) with their "Essential Eight" - a well-regarded and demonstrably effective set of cyber-defence actions that map very closely into the Critical Security Controls.

This Version of the Critical Security Controls

Feedback on Version 6 of the Controls (October 2015) was used this to drive the evolution of Version 7 to improve clarity and conciseness, as well as change emphasis. The new version enables greater manageable implementation, measurement, and automation.

1 Scope

The present document describes a specific set of technical measures available to detect, prevent, respond, and mitigate damage from the most common to the most advanced of cyber-attacks. The measures reflect the combined knowledge of actual attacks and effective defences.

The present document is technically equivalent and compatible with CIS Controls, Version 7.0 of the Center for Internet Cybersecurity [i.1].

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] The Center for Internet Cybersecurity: "CIS Controls™". Version 7.0 2018.

NOTE: Available at https://www.cisecurity.org/critical-controls.cfm.

[i.2] NIST Special Publication 800-57 (Part 1-Revision 4): "Recommendation for Key Management".

[i.3] IEEE 802.1X™ (2010): "Port Based Network Access Control".

[i.4] ETSI TR 103 305-2: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 2: Measurement and auditing".

[i.5] NIST Special Publication 800-63: "Digital Identity Guidelines".

[i.6] NIST Special Publication 800-50: "Building an Information Technology Security Awareness and Training Program".

[i.7] ENISA: "The new users' guide: How to raise information security awareness".

NOTE: Available at https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide.

[i.8] EDUCAUSE: "Cybersecurity Awareness Resource Library".

NOTE: Available at https://spaces.internet2.edu/display/2014infosecurityguide/Cybersecurity+Awareness+Resource+Library.

[i.9] SANS: "Security Awareness Reports & Resources".

NOTE: Available at https://www.sans.org/security-awareness-training/reports.

[i.10] ETSI TR 103 331: "CYBER; Structured threat information sharing".

[i.11] CREST: "Cyber Security Incident Response Guide".

NOTE: Available at https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf.

[i.12] CREST: "Guidance and standards on cyber defence topics".

NOTE: Available at https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf.

[i.13] PCI Security Standards Council.

NOTE: Available at https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf.

[i.14] OWASP Penetration Testing Methodologies.

NOTE: Available at https://www.owasp.org/index.php/Penetration_testing_methodologies.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Critical Security Control (CSC): specified capabilities that reflect the combined knowledge of actual attacks and effective defences of experts that are maintained by the Center for Internet Security

NOTE: Available at https://www.cisecurity.org/critical-controls.cfm.

quick win: actions that can be relatively easily taken with minimal resources that have a significant cyber security benefit

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ACK	ACKnowledge
ACL	Access Controls List
AES	Advanced Encryption Standard
ASD	Australian Signals Directorate
ASLR	Address Space Layout Randomization
BYOD	Bring Your Own Device
CCE™	Common Configuration Enumeration
CDM	Continuous Diagnostic and Mitigation
CIS	Center for Internet Security
CPE™	Common Platform Enumeration
CSAF	Common Security Advisory Framework (Technical Committee OASIS)
CSC	Critical Security Control or Capability
CVE®	Common Vulnerability Enumeration
CVRF	Common Vulnerability Reporting Framework
CVSS	Common Vulnerability Scoring System
DEP	Data Execution Prevention
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DLP	Data Loss Prevention
DMZ	DeMilitarized Zone
DNS	Domain Name System
EAP	Extensible Authentication Protocol
HSM	Hardware Security Modules
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
ID	IDentifier
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology

LAN	Local Area Network
MAC	Media Access Control
NAC	Network Access Control
NFC	Near-Field Communication
NIST	National Institute of Standards and Technology
OVAL®	Open Vulnerability and Assessment Language
OWASP	Open Web Application Security Project
PCI	Payment Card Industry
SANS	SysAdmin, Audit, Network, Security institute
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Program
SIEM	Security Information Event Management or Security Incident Event Management
SP	Special Publication
SPF	Sender Policy Framework
SQL	Structured Query Language
SYN	SYNchronize
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAF	Web Application Firewall
WIDS	Wireless Intrusion Detection System
WLAN	Wireless Local Area Network
XCCDF	eXtensible Configuration Checklist Description Format

NOTE: CPE®, CVE™, OVAL® and CCE™ are trademarks of The MITRE Corporation operating as a non-profit Federally Funded Research and Development Center (FFRDC) of the U.S. Department of Homeland Security. See http://stixproject.github.io/legal/. Both CVE® and OVAL® are registered service marks. This information is given for the convenience of users of the present document and does not constitute an endorsement by ETSI of the product named. Equivalent products may be used if they can be shown to lead to the same results.

4 Critical Security Controls

4.0 Structure of the Critical Security Controls Document

The Critical Security Controls in the present document are organized as shown in figure 4-0. Controls 1 through 6 are essential to success and should be considered among the very first things to be done.

Figure 4-0: Organization of the Critical Security Controls

As depicted in figure 4-0, Controls 17-20 are different in character than Controls 1-16. While they have many technical elements, these are less focused on technical as controls and more focused on people and processes. They are pervasive in that they should be considered across the entire enterprise, and across all of Controls 1-16. Their measurements and metrics of success are driven more by observations about process steps and outcomes, and less by technical data gathering. They are also complex topics in their own right, each with an existing body of literature and guidance. For Controls 17-20, a small number of elements are identified that are critical to an effective program in each area. Processes and resources are described which can be used to develop a more comprehensive enterprise treatment of each topic. Both commercial and non-profit resources are identified. The ideas, requirements, and processes expressed in the references are well supported by the marketplace.

Each Control includes:

- A description of the importance of the Control (Why is This Control Critical) in blocking or identifying presence of attacks and an explanation of how attackers actively exploit the absence of this control.
- A table of the specific actions ("sub-controls") that organizations should take to implement, automate, and measure effectiveness of the control.
- Procedures and Tools that enable implementation and automation.
- Sample Entity Relationship Diagrams that show components of implementation.

In addition to the present document, ETSI TR 103 305-2 [i.4], can be referenced for implementing each control.

4.1 CSC 1: Inventory and Control of Hardware Assets

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Why Is This Control Critical?

Attackers, who can be located anywhere in the world, are continuously scanning the address space of target organizations, waiting for new and possibly unprotected systems to be attached to the network. They are particularly interested in devices which come and go off of the enterprise's network such as laptops or Bring-Your-Own-Devices (BYOD) which might be out of synch with security updates or might already be compromised. Attacks can take advantage of new hardware that is installed on the network one evening but not configured and patched with appropriate security updates until the following day. Even devices that are not visible from the Internet can be used by attackers who have already gained internal access and are hunting for internal pivot points or victims. Additional systems that connect to the enterprise's network (e.g. demonstration systems, temporary test systems, guest networks) should also be managed carefully and/or isolated in order to prevent adversarial access from affecting the security of enterprise operations.

Large, complex enterprises understandably struggle with the challenge of managing intricate, fast-changing environments. But attackers have shown the ability, patience, and willingness to "inventory and control" our assets at very large scale in order to support their opportunities.

Managed control of all devices also plays a critical role in planning and executing system backup, incident response, and recovery .

Table 4-1: CSC 1 - Inventory and Control of Hardware Assets

Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions
1.1	Devices	Identify	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.
1.2	Devices	Identify	Use a Passive Asset Discovery Tool	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.
1.3	Devices	Identify	Use DHCP Logging to Update Asset Inventory	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.
1.4	Devices	Identify	Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory should include all hardware assets, whether connected to the organization's network or not.
1.5	Devices	Identify	Maintain Asset Inventory Information	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.
1.6	Devices	Respond	Address Unauthorized Assets	Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.
1.7	Devices	Protect	Deploy Port Level Access Control	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system should be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.
1.8	Devices	Protect	Utilize Client Certificates to Authenticate Hardware Assets	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.

CSC 1: Procedures and Tools

This Control includes both technical and procedural actions, united in a process that accounts for and manages the inventory of hardware and all associated information throughout its life cycle. It links to business governance by establishing information/asset owners who are responsible for each component of a business process that includes information, software, and hardware. Organizations can use large-scale, comprehensive enterprise products to maintain IT asset inventories. Others use more modest tools to gather the data by sweeping the network, and manage the results separately in a database.

Maintaining a current and accurate view of IT assets is an ongoing and dynamic process. Organizations can actively scan on a regular basis, sending a variety of different packet types to identify devices connected to the network. Before such scanning can take place, organizations should verify that they have adequate bandwidth for such periodic scans by consulting load history and capacities for their networks. In conducting inventory scans, scanning tools could send traditional ping packets (e.g. ICMP Echo Request) looking for ping responses to identify a system at a given IP address. Because some systems block inbound ping packets, in addition to traditional pings, scanners can also identify devices on the network using transmission control protocol (TCP) synchronize (SYN) or acknowledge (ACK) packets. Once they have identified IP addresses of devices on the network, some scanners provide robust fingerprinting features to determine the operating system type of the discovered machine.

In addition to active scanning tools that sweep the network, other asset identification tools passively listen on network interfaces for devices to announce their presence by sending traffic. Such passive tools can be connected to switch span ports at critical places in the network to view all data flowing through such switches, maximizing the chance of identifying systems communicating through those switches.

Many organizations also pull information from network assets such as switches and routers regarding the machines connected to the network. Using securely authenticated and encrypted network management protocols, tools can retrieve MAC addresses and other information from network devices that can be reconciled with the organization's asset inventory of servers, workstations, laptops, and other devices. Once MAC addresses are confirmed, switches should implement 802.1x and NAC to only allow authorized systems that are properly configured to connect to the network [i.3].

Wireless devices (and wired laptops) may periodically join a network and then disappear, making the inventory of currently available systems very dynamic. Likewise, virtual machines can be difficult to track in asset inventories when they are shut down or paused. Additionally, remote machines accessing the network using virtual private network (VPN) technology may appear on the network for a time, and then be disconnected from it. Whether physical or virtual, each machine using an IP address should be included in an organization's asset inventory.

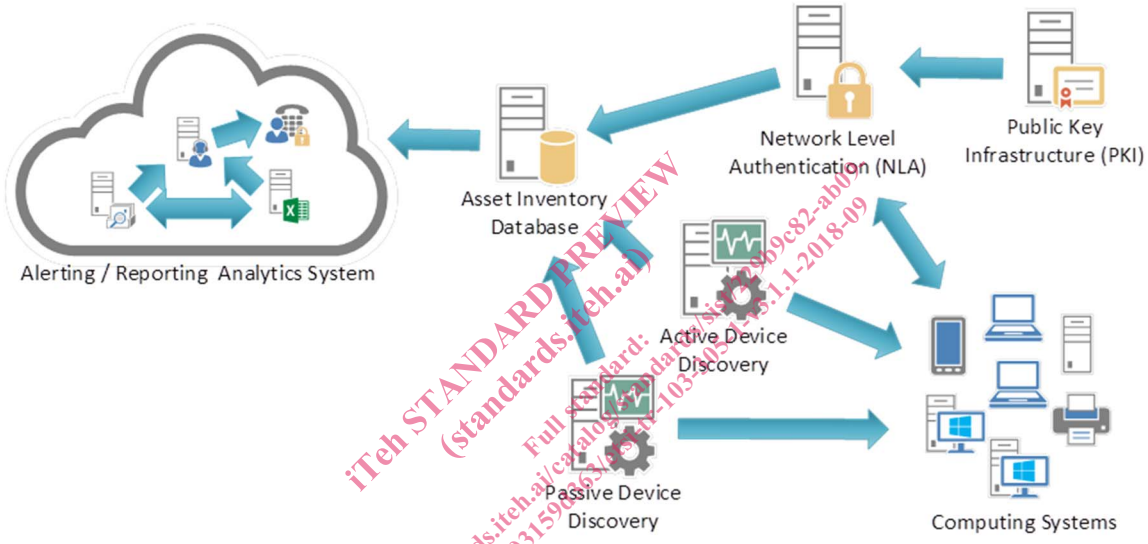

Figure 4-1: CSC 1 System Entity Relationship Diagram

4.2 CSC 2: Inventory and Control of Software Assets

Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Why Is This Control Critical?

Attackers continuously scan target organizations looking for vulnerable versions of software that can be remotely exploited. Some attackers also distribute hostile web pages, document files, media files, and other content via their own web pages or otherwise trustworthy third-party sites. When unsuspecting victims access this content with a vulnerable browser or other client-side program, attackers compromise their machines, often installing backdoor programs and bots that give the attacker long-term control of the system. Some sophisticated attackers may use zero-day exploits, which take advantage of previously unknown vulnerabilities for which no patch has yet been released by the software vendor. Without proper knowledge or control of the software deployed in an organization, defenders cannot properly secure their assets.

Poorly controlled machines are more likely to be either running software that is unneeded for business purposes (introducing potential security flaws), or running malware introduced by an attacker after a system is compromised. Once a single machine has been exploited, attackers often use it as a staging point for collecting sensitive information from the compromised system and from other systems connected to it. In addition, compromised machines are used as a launching point for movement throughout the network and partnering networks. In this way, attackers may quickly turn one compromised machine into many. Organizations that do not have complete software inventories are unable to find systems running vulnerable or malicious software to mitigate problems or root out attackers.

Managed control of all software also plays a critical role in planning and executing system backup, incident response and recovery.

Table 4-2: CSC 2 - Inventory and Control of Software Assets

Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions
2.1	Applications	Identify	Maintain Inventory of Authorized Software	Maintain an up-to-date list of all authorized software that is necessary in the enterprise for any business purpose on any business system.
2.2	Applications	Identify	Ensure Software is Supported by Vendor	Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.
2.3	Applications	Identify	Utilize Software Inventory Tools	Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.
2.4	Applications	Identify	Track Software Inventory Information	The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the organization.
2.5	Applications	Identify	Integrate Software and Hardware Asset Inventories	The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.
2.6	Applications	Respond	Address Unapproved Software	Ensure that unauthorized software is either removed or the inventory is updated in a timely manner.
2.7	Applications	Protect	Utilize Application Whitelisting	Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.
2.8	Applications	Protect	Implement Application Whitelisting of Libraries	The organization's application whitelisting software should ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc.) are allowed to load into a system process.
2.9	Applications	Protect	Implement Application Whitelisting of Scripts	The organization's application whitelisting software should ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc.) are allowed to run on a system.
2.10	Applications	Protect	Physically or Logically Segregate High Risk Applications	Physically or logically segregated systems should be used to isolate and run software that is necessary for business operations but incur higher risk for the organization.

CSC 2: Procedures and Tools

Whitelisting can be implemented using a combination of commercial whitelisting tools, policies or application execution tools that come with anti-virus suites and popular operating systems. Commercial software and asset inventory tools are widely available and in use in many enterprises today. The best of these tools provide an inventory check of hundreds of common applications used in enterprises, pulling information about the patch level of each installed program to ensure that it is the latest version and leveraging standardized application names, such as those found in the common platform enumeration specification.